| Cybersecurity |
| --- |
| 21.3 The Final Report |

Case Report

National Gallery DC

### Tracy’s iPhone [2012-07-15-National-Gallery]

Charles Wallace

May 23, 2023

# Table of Contents

[Case Report](#_8mjg1w2w81ai)

[National Gallery DC](#_lrib8gqk2z7b)

[Tracy’s iPhone [2012-07-15-National-Gallery]](#_219o4hryceis)

[Table of Contents](#_786gzvga2e8h)

[Executive Summary](#_ccs3x82xm1tu)

[Equipment and Tools](#_hw4rzs3hh4tn)

[Details of Tracy’s iPhone](#_ebsdggfieq5h)

[Evidence to Establish Personas](#_qixiazcd0tiw)

[Evidence relating to theft of valuable stamps](#_5ri2s3hfb3bw)

[Evidence relating to defacement of museum art](#_kt32233q8aao)

[Plot Timeline](#_nz1crxu2ypd4)

[Conclusion](#_m5r3zcqmj9ou)

Appendix A: [Correspondence Evidence](#_w4pkinqwxqi8)

Appendix B: [WiFi and GPS Location Information](#_f8fx30pgaw29)

# Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

* Tracy is a suspect in the aforementioned conspiracy.
* As part of the investigation, Tracy’s iPhone was taken into custody.
* Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

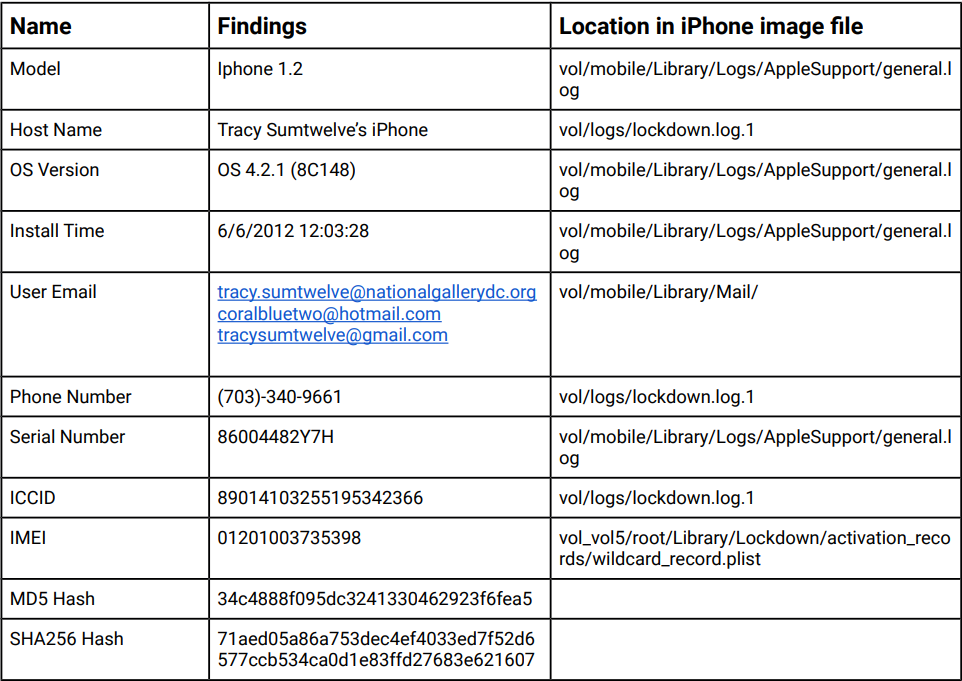
As described fully in the report, Digitech, Inc. made the following findings.

Evidence was uncovered that Tracy, a supervisor at the National Gallery who is motivated by financial gain, planned a heist targeting stamps from the National Gallery. During the investigation, evidence was uncovered that supports the following findings: Tracy was using the alias Coral and that Pat was using the alias Perry. Tracy was motivated by financial gain in planning the stamp heist due to running into money troubles mainly centering around her daughter's school tuition. Emails originating from Tracy’s and Pat’s personal emails contain details of the National Gallery DC stamp letters. Digitech Inc. found evidence indicating that Tracy was forming a plan to steal stamps with Pat’s assistance. Additionally, Digitech Inc. found evidence that indicated Tracy knew that Pat was blackmailing someone named King to help them with the heist and to provide supplies. Digitech Inc., also found evidence indicating Tracy helped an individual named Carry for financial gain. The evidence included leaked sensitive security rotation information for the National Gallery to Carry. There is also evidence implicating that Tracy helped smuggle a tablet into the National Gallery for Carry. Also found in “Notes” under the library, that Tracy took note of needing to find “help” for Prufrock, which is the school that her daughter Terry attends. (Note aforementioned financial troubles) Also found a search for “Financial Aid” in Tracy’s Safari Cache.

### Equipment and Tools

* Autopsy
* Kali Linux
* SQLite Browser (DB Browser for SQLite)
* Google Maps/Google Earth
* Nano (text editor)
* Note Pad (text editor)

# Details of Tracy’s iPhone



# Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy: Alias: Coral Blue

Phone Number: (703) 340-9961

Personal Email: tracysumtwelve@gmail.com

Work Email: tracy.sumtwelve@nationalgallerydc.org

Alias Email: coralbluetwo@hotmail.com

Relationship: Accused

Pat: Alias: Perry

Phone Number: (571) 308-3236

Email: patsumtwelve@gmail.com

Relationship: Tracy’s brother

Terry:

Phone Number: (703) 829-6071

Email: N/A

Relationship: Tracy and Joe’s daughter

Joe:

Phone Number: N/A

Email: joe.sum.twelve@gmail.com

Relationship: Tracy’s ex-husband and Terry’s Father

Carry: Alias: Cat

Phone Number: (202) 725-2124

Email: catsumtwelve@gmail.com

Relationship: An acquaintance of Tracy’s

Through the investigation the data that was collected is from Tracy’s iPhone, and the email associated with the Apple ID is ‘[tracysumtwelve@gmail.com](mailto:tracysumtwelve@gmail.com)’. Also, her work email ‘[tracy.sumtwelve@nationalgallerydc.org](mailto:tracy.sumtwelve@nationalgallerydc.org)’ was setup on this phone, along with another email address under the alias of Coral Blue. Tracy is a supervisor at the NGDC. She is colluding with her brother, Pat (Perry), and his accomplice, King (Kart), to steal stamps at the NGDC. She is also getting help from her colleague Carry (Cat) at NGDC to get some pictures on a tablet.

# Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

Tracy came across the valuable stamp collection exhibit as shown in ‘Mailbox Data Structure’. Tracy (Coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she believes that it would be a big deal. They also show Tracy and Pat being interested in stealing it since it’s small and valuable. Pat tries to enroll someone by the name of King via blackmail, as he is currently on parole. King agrees to be a part of the heist and sends out a list of required supplies. Pat then forwards the list to Tracy along with instructions on how to access the attachment over SMS, which Tracy then acknowledges. Tracy also emails the insurance documents regarding the stamp collection exhibit which were marked as confidential to Pat. Tracy’s iPhone also has multiple photos of the stamps mentioned in the insurance documents. All these pieces of evidence make it clear that Pay and Tracy were conspiring to steal valuable stamps.

Images from Tracy’s iPhone show photos of Gallery Stamps. These were taken prior to the heist. The Geo-Location information for these images shows that they were taken at the Museum, proving that Tracy took them while there. We think that this is important information leading to the accusation that she may have been sending them to people or taking them to show people later on.

Photos



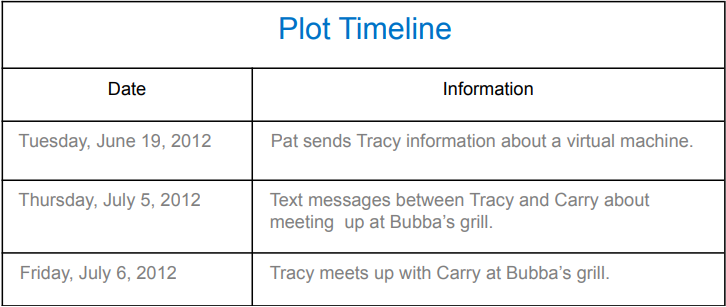
# Evidence relating to defacement of museum art

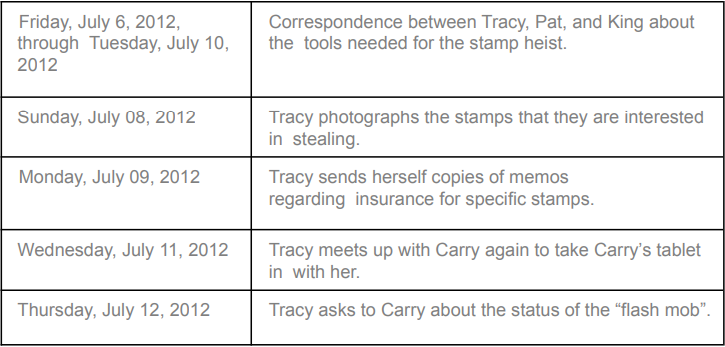
This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

Carry reached out to Tracy, they met over lunch. In the same email, Carry asks Tracy for help with sneaking a tablet into the National Gallery for a flash mob event that she was planning. Carry also mentions that she would compensate Tracy for her help. Tracy agrees to sneak the tablet in and a meeting is set for the hand-off at 9. Also, Carry asked for information on the security shift change schedule. Tracy receives notifications from Google+ informing her that Carry added her to a circle and that she shared something with her on Google+. In one of these notifications was the suggestion to add Alex JFamEleven who was a part of Carry’s circles. Tracy messaged Carry asking how the flash mob was going. This message and earlier communication together present a view that Tracy, although a part in leaking information and smuggling in the tablet, was not aware of anything additional in the plot for defacing art at the museum.

# Plot Timeline

* Email Content: /mobile/Library/Mail/Protected\_Indexed
* SMS Content: /mobile/Library/SMS/sms.db
* Call Data: /wireless/Library/CallHistory/call\_history.db
* Wifi & Cell Location Data: /root/Library/Caches/locationd/consolidated.db





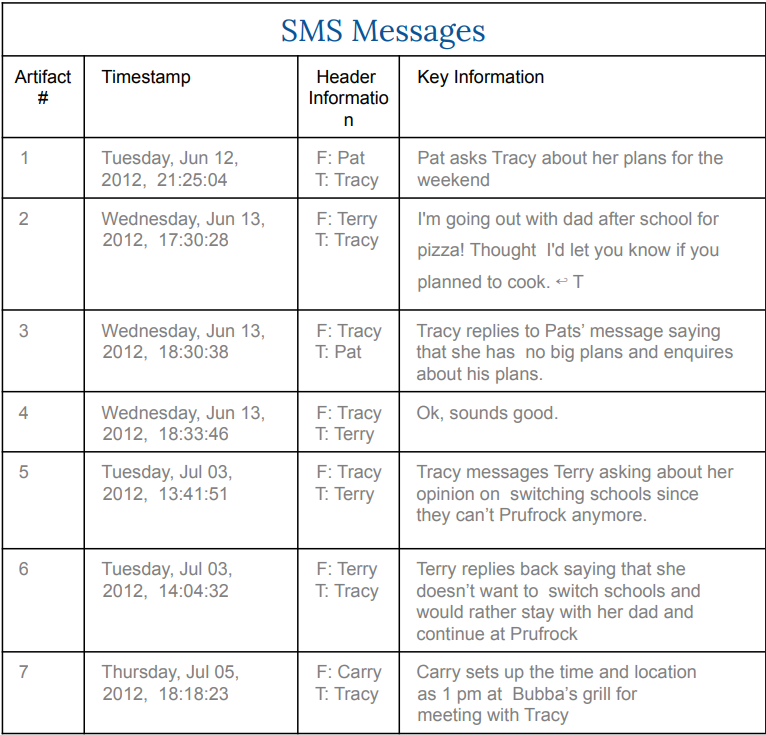
# Conclusion

Evidence found on Tracy’s iPhone indicated the following:

* Tracy used the alias Coral and Pat used the alias Perry.
* Tracy’s prime motive was financial gain for planning the stamp heist.
* Tracy emailed National Gallery DC stamp letters to her personal email account and to Pat.
* Tracy formulated a plan with Pat to steal stamps from NGDC.
* Tracy knew that Pat was blackmailing someone named Kind to help with the heist.
* Tracy helped Carry also, for financial gain.
* Tracy leaked sensitive security rotation information about the National Gallery to Carry.
* Tracy helped Carry smuggle a tablet into the Gallery.
* Tracy was unaware of the bigger plan that Carry was a part of.

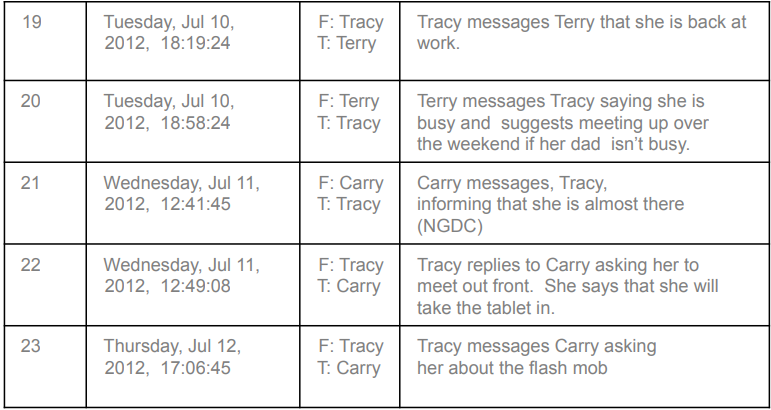
# Appendix A: Correspondence Evidence

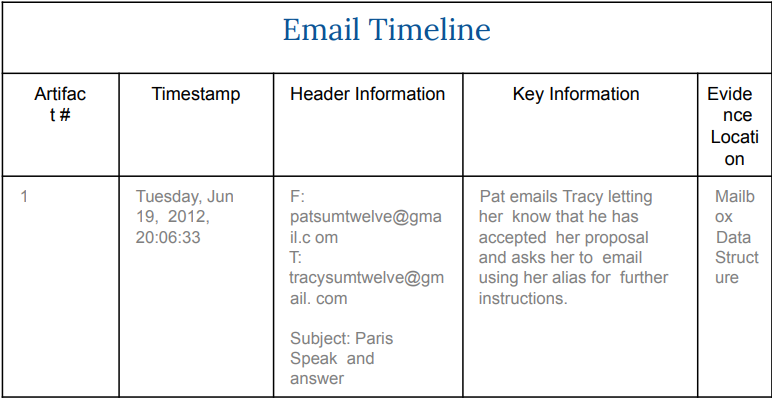
This subsection will provide an amalgamation of the email and SMS correspondence evidence.

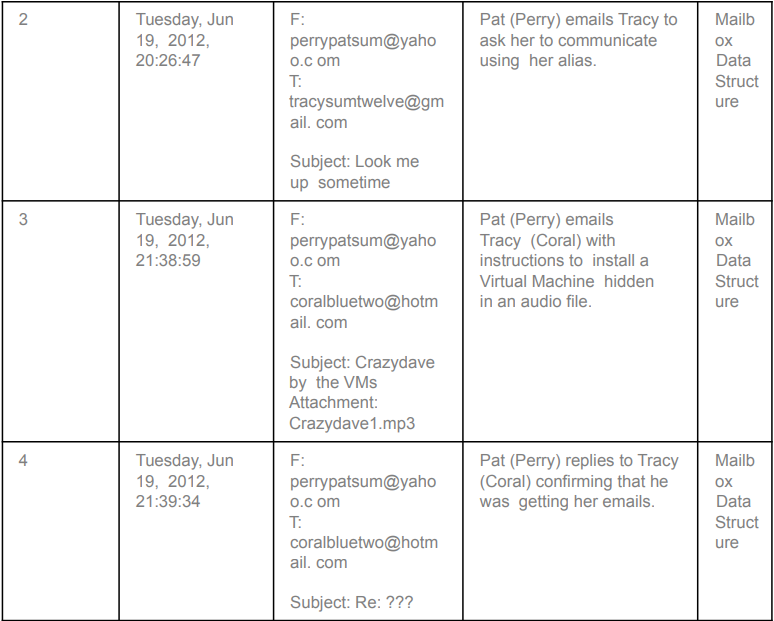


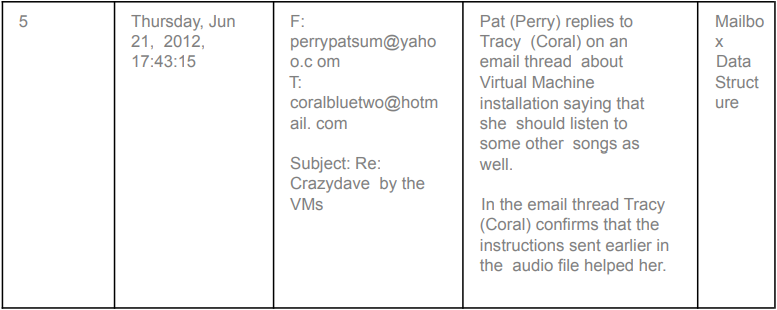


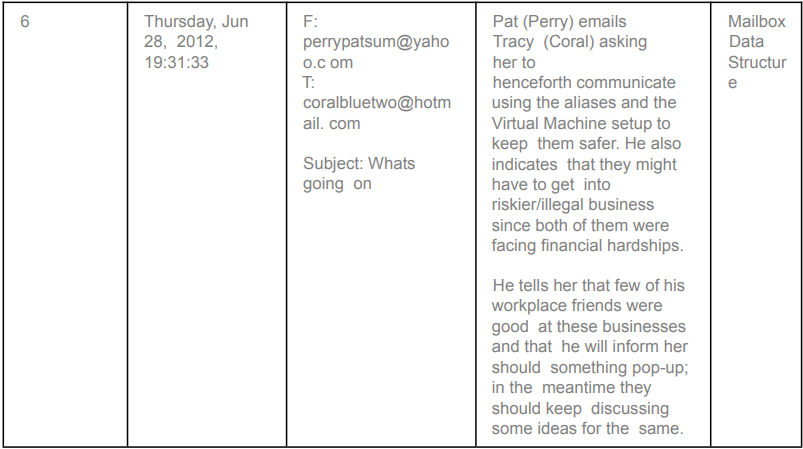


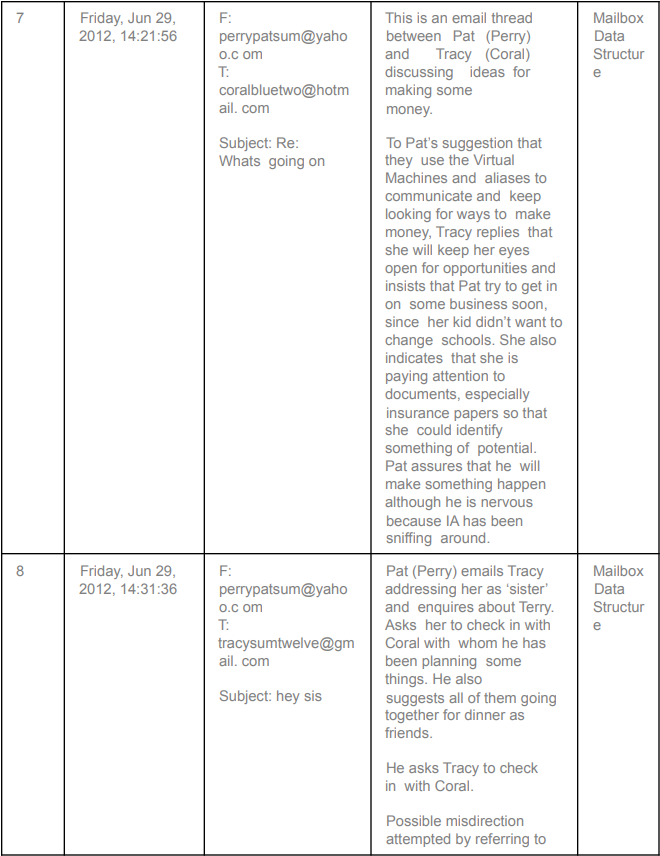


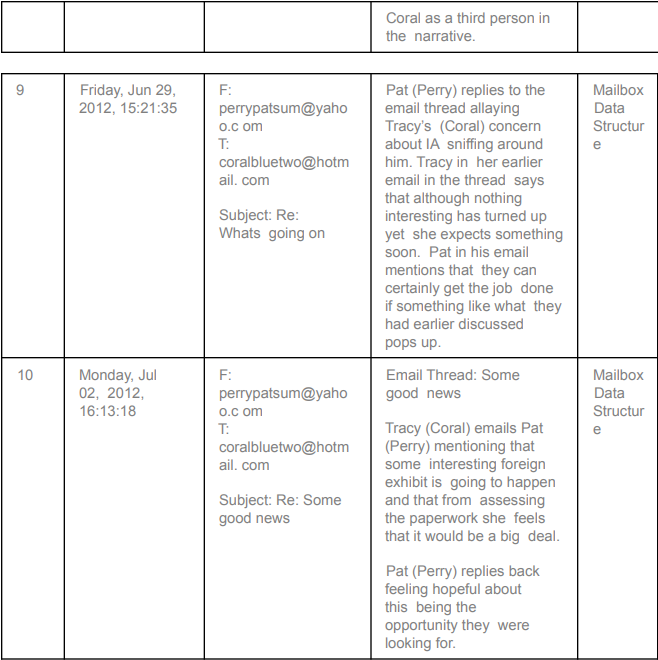


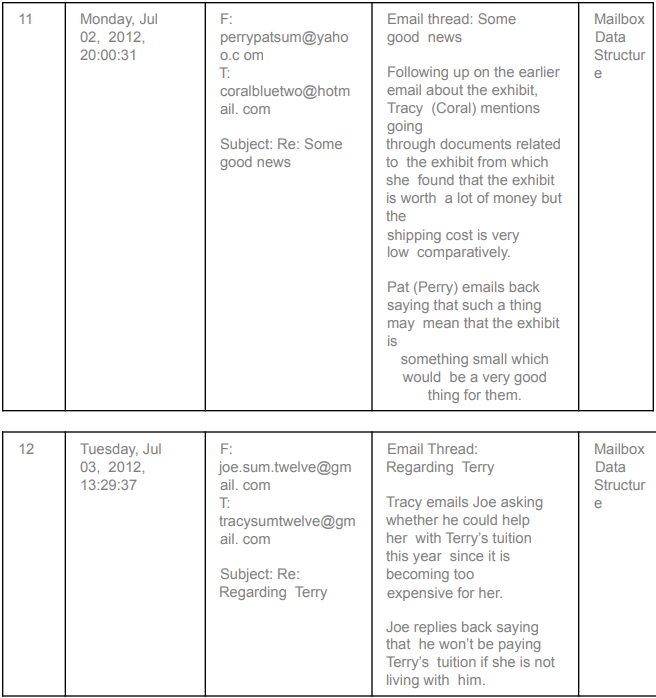


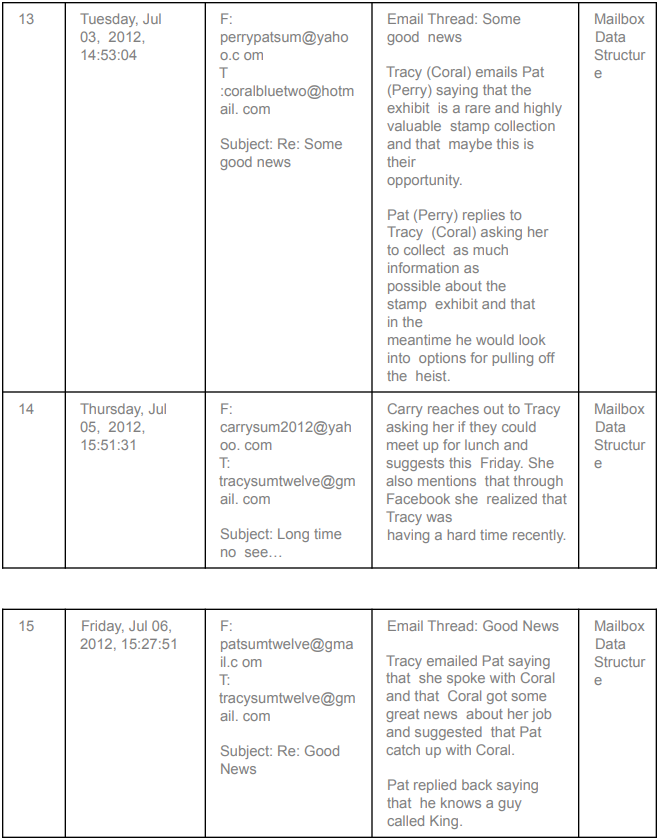


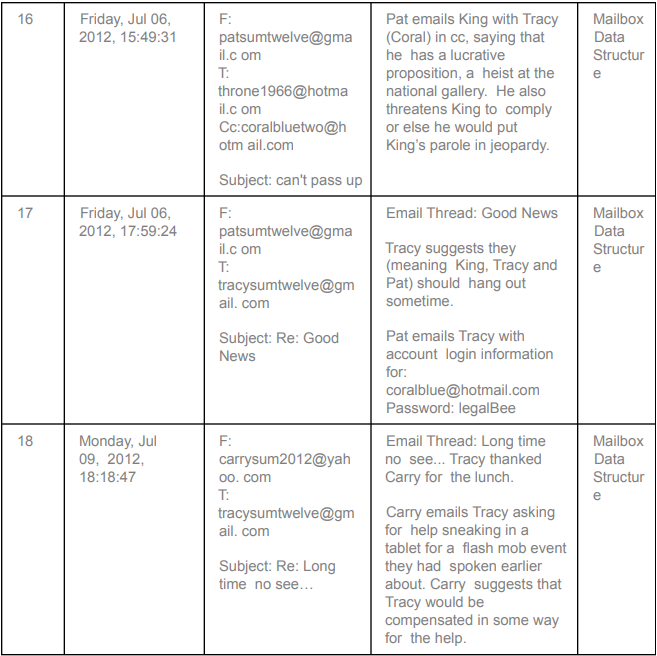


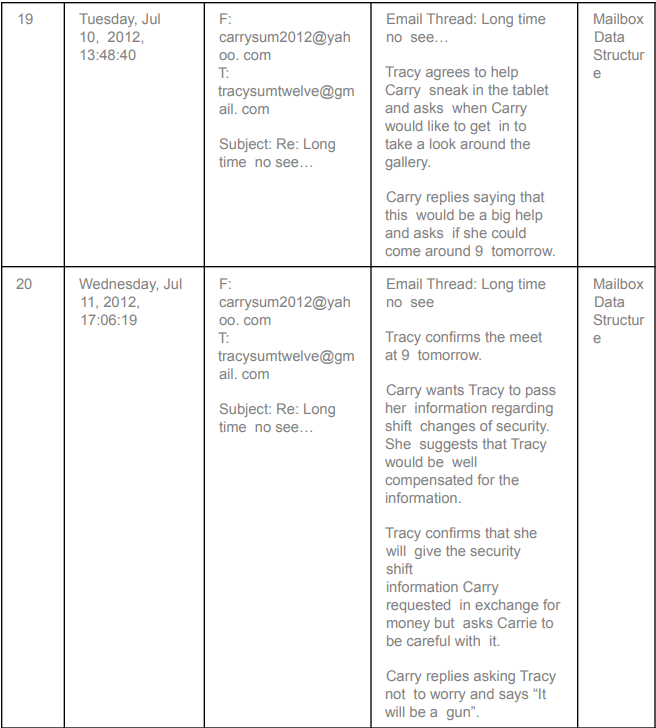


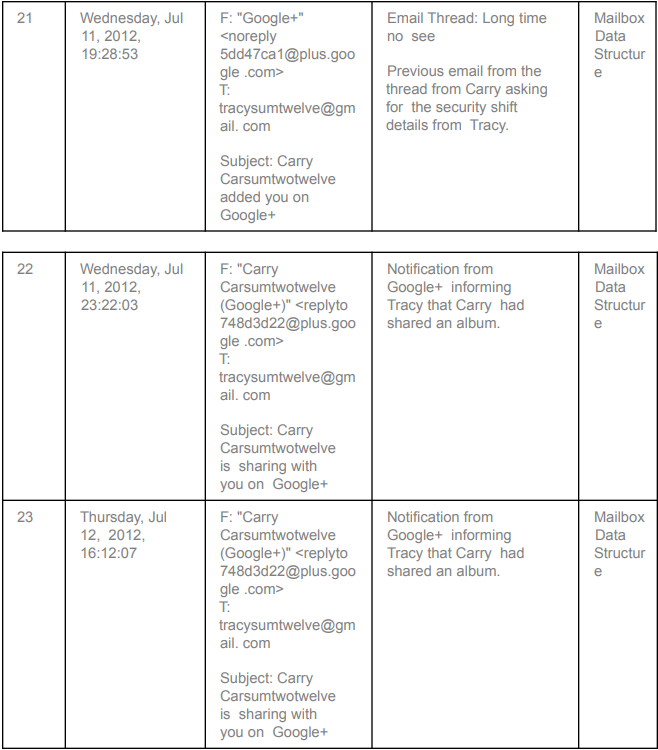














# Appendix B: WiFi and GPS Location Information

